



(WO/2004/042602) APPARATUS TO IMPLEMENT DUAL HASH ALGORITHM

[Biblio. Data](#) [Description](#) [Claims](#) [National Phase](#) [Notices](#) [Documents](#)

Latest bibliographic data on file with the International Bureau

Publication Number: WO/2004/042602 **International Application No.:** PCT/SG2002/000245
Publication Date: 21.05.2004 **International Filing Date:** 21.10.2002
Chapter 2 Demand Filed: 27.04.2004

Int. Class.: H04L 9/32 (2006.01)

Applicants: STMICROELECTRONICS ASIA PACIFIC PTE LTD. [SG/SG]; 28 Ang Mo Kio Industrial Park 2, Singapore 569508 (SG) (*All Except US*).

PLESSIER, Bernard [FR/SG]; 25 Leonie Hill Road, #06-05 Grangeford, Singapore 239196 (SG) (*US Only*).

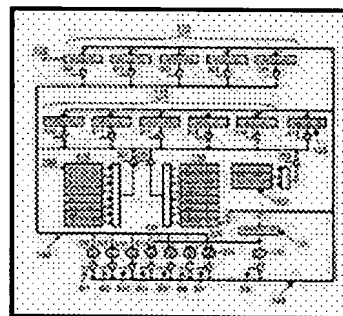
MING, Kiat. Yap [MY/SG]; Blk 248, Jurong East Street 24, #11-62, Singapore 600248 (SG) (*US Only*).

Inventors: PLESSIER, Bernard [FR/SG]; 25 Leonie Hill Road, #06-05 Grangeford, Singapore 239196 (SG).
 MING, Kiat. Yap [MY/SG]; Blk 248, Jurong East Street 24, #11-62, Singapore 600248 (SG).

Agent: DONALDSON & BURKINSHAW; P.O. Box 3667, Singapore 905667 (SG).

Title: APPARATUS TO IMPLEMENT DUAL HASH ALGORITHM

Abstract: Apparatus is disclosed which is arranged to accept digital data as an input, and to process said data according to one of either the Secure Hash Algorithm (SHA-1) or Message Digest (MD5) algorithm to produce a fixed length output word. The apparatus includes a plurality of rotational registers for storing data, one of the registers being arranged to receive the input data, and data stores for initialisation of some of said plurality of registers according to whether the SHA-1 or MD5 algorithm is used. The data stores include fixed data relating to SHA-1 and MD5 operation. Also included is a plurality of dedicated combinatorial logic circuits arranged to perform logic operations on data stored in selected ones of said plurality of registers.



Designated JP, SG, US.

States: European Patent Office (EPO) (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

Publication Language: English (EN)

Filing Language: English (EN)

DUAL HASH ALGORITHM IMPLEMENTATION

Background of the invention

- 5 The present invention relates to an efficient hardware implementation of the Secure Hash Algorithm (SHA-1) and Message Digest Algorithm (MD5).

Description of the Prior Art

- 10 Hash algorithms and message digests are frequently used in applications such as digital signatures, where it is desirable to verify the authenticity of a document or file. Techniques for producing message digests are beneficial as they reduce the amount of data processing needed to a manageable and consistent level.

- 15 The Secure Hash algorithm (SHA-1) is specified in Secure Hash Standard (FIPS PUB 180-1), and is an algorithm which operates on an input data file to produce a condensed representation of that file. Specifically, an message of arbitrary length is processed to produce a message digest consisting of exactly 160 bits.

- 20 The Message Digest Algorithm (MD5), developed by Professor Ronald Rivest, has a similar function. It accepts inputs of arbitrary length and produces an output message digest consisting of exactly 128 bits.

- 25 Both algorithms may be used as a constituent part of a digital signature application. Both algorithms are computationally intensive and, when implemented in software, as is the norm in prior art systems, can take a great number of processor clock cycles to complete.

- 30 The present invention therefore aims to overcome problems with the prior art implementation of these systems, particularly in relation to speed of operation and power consumption.

Summary of the Present Invention

In a first broad form the present invention provides apparatus arranged to accept digital data as an input, and to process said data according to one of either the

Secure Hash Algorithm (SHA-1) or Message Digest (MD5) algorithm to produce a fixed length output word, said apparatus including: a plurality of rotational registers for storing data, one of said registers being arranged to receive the input data; and data stores for initialisation of some of said plurality of registers according to whether
5 the SHA-1 or MD5 algorithm is used, said data stores including fixed data relating to SHA-1 and MD5 operation; and a plurality of dedicated combinatorial logic circuits arranged to perform logic operations on data stored in selected ones of said plurality of registers.

10 Preferably, the register arranged to receive the input data is arranged to receive said input data serially.

Preferably, the registers and combinatorial logic circuits are interconnected for communication via a pair of data busses. It is particularly preferable if the registers
15 and combinatorial logic circuits are connected to write to a respective bus via respective tristate buffers.

Preferably, the apparatus includes a control circuit arranged to generate individually gated clock signals for each register. This results in lower power consumption as
20 only active registers need to be clocked.

Preferably, the control circuit is further arranged to generate individual enabling signals to control the tristate buffers. The control circuit may be implemented as a dedicated state machine, or by another means such as a microcontroller.
25

Preferably, the rotational registers are arranged to be multiplexed prior to connection to a tristate buffer. This results in a lower bus loading.

Preferably, the combinatorial logic circuits include a copy circuit, a shift left circuit, a
30 NOT circuit, an ADD circuit, an OR circuit, an AND circuit and an XOR circuit. Each circuit is dedicated to its particular task, avoiding redundancy.

Preferably, the apparatus is implemented as an integrated circuit, typically of the ASIC type. The apparatus may be incorporated with other apparatus, typically digital signature apparatus.

5

Embodiments of the present invention utilise the fact that both algorithms may be broken down into a series of individual steps. Prior art approaches to implementing the algorithms in software do not utilise any specialised hardware components, which results in a relatively slow process. However, embodiments of the invention

10 identify, where possible, the common elements between the MD5 and SHA-1 algorithms and provide specialised hardware components to achieve the required functionality. Hardware is selected which allows for the maximum sharing of components and hence the minimum overall component count.

15

Embodiments of the present invention allow a relatively small number of dedicated components to be used in a circuit to efficiently calculate either MD5 or SHA-1 message digests. Since the operations involved in both algorithms are similar, the circuit can be optimised to allow components which are common to both algorithms to be provided only once. Allowing either of the algorithms to be used in calculating

20 a message digest is advantageous as there are several digital signature systems operational which make use of one or other of the SHA-1 or MD5 algorithms. Systems utilising an embodiment of the invention benefit from increased flexibility and speed.

25

Brief Description of the Drawings

For a better understanding of the present invention and to understand how the same may be brought into effect, the invention will now be described by way of example only, with reference to the appended drawings in which:

30

Figure 1 shows a view of the architecture of the combined SHA-1 and MD5 processor; and

Figure 2 shows a view of the control circuit used to control the architecture shown in Figure 1.

Detailed Description of the Preferred Embodiments

Figure 1 shows a customised architecture which is arranged to receive a data input 150, process it using the shown elements, and produce a data output 155. The hardware shown is able to perform either SHA-1 or MD5 processing on the input data, and has been optimised in order to minimise the amount of hardware needed to perform either one of the algorithms.

The circuit includes a plurality of registers for storing data. There are ten registers provided in two banks 110, 115 for storing part of the data being processed. In addition, two temporary registers 120, 135 are provided for intermediate processing and temporary storage. Also provided are two banks 125, 130 of circular shift registers W15[31:0] – W0[31:0]. Register W15 of bank 125 is arranged to receive the input data 150. Any data held in W15 at that time is shifted to W14; the data in W14 is shifted to W13 and so on, until the data held in W0 is lost. The outputs of banks 125 and 130 are multiplexed before being attached to the read bus 140 by a tristate buffer in order to reduce bus loading.

The registers are mutually interconnected for communication via a read bus 140 and a write bus 145.

The read bus 140 is connected to a range of logic circuits which provide combinatorial functions. These functions are: Copy (CP) 200, Shift Left multiple positions (SL*) 205, NOT 210, ADD 215, OR 220, AND 225, XOR 230 and Shift Left one position (SL1) 235. Functions 200, 205, 210 require only a single input variable and receive it directly from the read bus 140. The other functions 215, 220, 225 and 230 require two input variables and receive one from the read bus 140 and the other from a temporary register (ACCU[31:0]) 135. Register 135 also provides the input for shift register 235.

Also connected to the read bus via a multiplexer and a tristate logic gate is a bank 160 of registers including fixed constants used in the initialisation of the circuit for either SHA-1 or MD5 mode calculations. K[t] is provided for initialisation of SHA-1, and T[i] is provided for initialisation of MD5. In total, approximately seventy five

constants each having a length of 32 bits are required, and grouping them together in this fashion allows them to be conveniently accessed. The synthesis tool which places the gates in the finished custom device is then able to optimise the logic, resulting in a smaller gate count, and thus a smaller area of silicon is required.

5

Calculation of either SHA-1 or MD5 requires the use of selected ones of the provided registers and combinatorial functions. In particular, calculation of the SHA-1 algorithm uses all the registers of bank 110 and of bank 115. Calculation of MD5 requires only the use of four registers (H0 – H3) of bank 110 and four registers (A-D) of bank 115. This allows the unused registers to be used for temporary storage if required. However, when the result of the calculation 155 is unloaded from register H0 of bank 110, all five registers are read since they are implemented as shift registers, and this ensures that their contents are unchanged.

15 All devices which can output data to the read bus 140 are connected to the bus via a tristate buffer. Each buffer is individually enabled via a control signal created by the control circuit shown in Figure 2. Likewise, the combinatorial functions 200-235 which can write data onto the write bus 145 are connected to the write bus via individually controllable tristate buffers.

20

The group of clock signals 345 to individual registers are created from a master clock signal 340. The master clock signal is ANDed with a control signal to create a gated clock signal for the appropriate register. In this way, the energy consumption of the complete circuit is reduced as only active registers need to be clocked.

25

Figure 2 shows the a top level view of the control circuit 400 which generates the various control signals for the circuit of Figure 1. In particular, it generates, from a master clock signal 340, a series 345 of gated individual clock signals which are used to clock the various registers of Figure 1. It also generates individual enable signals for each of the tristate buffers shown in Figure 1. The control circuit may take the form of a finite state machine including associated controlling circuits.

30

The following pseudo-code represents the steps performed in calculating a message digest according to the SHA-1 algorithm on an input data word of arbitrary length.

The high level algorithm details in broad terms the steps taken in performing a calculation according to the SHA-1 algorithm. The following more detailed code provides step by step instructions on performing the individual instructions needed to calculate the message digest.

5

SHA-1 Algorithm

// High Level Algorithm

initialize SHA-1 internal registers (H0,H1,H2,H3,H4)

10 foreach Mi, block of 512 bits of M do

load Mi into data registers W[0] to W[15]

start core SHA-1

end

unload H0,H1,H2,H3,H4

15

//Detailed steps

SHA-1 initialization

20 H0 = 67452301

H1 = EFCDAB89

H2 = 98BADCFE

H3 = 10325476

H4 = C3D2E1F0

25

Core SHA-1

A=H0, B=H1, C=H2, D=H3, E=H4

MASK=0000000F

for t=0 to 79 do

30 s = t and MASK;

if (t>=16) W[s] = SL1(W[(s + 13) and MASK] xor

W[(s + 8) and MASK] xor

W[(s + 2) and MASK] xor W[s]);

end if

-7-

```

TEMP = SL5(A) + ft(B,C,D) + E + W[s] + K[t]
E=D, D=C, C=SL30(B), B=A, A=TEMP
end for
H0 =H0+A, H1 =H1+B, H2 =H2+C, H3=H3+D, H4=H4+E
5
// The functions SL1, SL5 and SL30 are circular left rotation
// of the 32 bit operand by 1 bit, 5 bits and 30 bit
// respectively.
// The constants Kt are defined by the following:
10
Kt = 5A82 7999 ( 0 <= t <= 19)
Kt = 6ED9 EBA1 (20 <= t <= 39)
Kt = 8F1B BCDC (40 <= t <= 59)
Kt = CA62 C1D6 (60 <= t <= 79).
15
// The functions ft(B,C,D) is defined by the following:
ft (B,C,D) = (B and C) or ((not B) and D) (0 <= t <= 19)
ft (B,C,D) = B xor C xor D (20 <= t <= 39)
ft (B,C,D) = (B and C) or (B and D) or (C and D) (40 <= t <=
20 59)
ft (B,C,D) = B xor C xor D (60 <= t <=79).

```

25 The following pseudo-code represents the steps performed in calculating a message digest according to the MD5 algorithm on an input data word of arbitrary length.

MD5 Pseudo Algorithm

```

// Here, the four auxiliary functions that each take as input
// three 32-bit words and produce as output one 32-bit word
30 // are defined:

```

```

F(X,Y,Z) = (X and Y) or (not(X) and Z)
G(X,Y,Z) = (X and Z) or (Y and not(Z))
H(X,Y,Z) = X xor Y xor Z

```


$I(X,Y,Z) = Y \text{ xor } (X \text{ or } \text{not}(Z))$

// A 64-element table T[1 ... 64] constructed from the sine
 // function is defined. Let T[i] denote the i-th element of
 5 // the table, which is equal to the integer part of 4294967296
 // times abs(sin(i)), where i is in radians.

High Level Algorithm

initialize MD5 internal registers (H0,H1,H2,H3)
 10 foreach Mi, block of 512 bit of M do
 load Mi into data registers W[0] to W[15]
 start core MD5
 end
 unload H0, H1, H2, H3

15 MD5 initialization

H0 = 67 45 23 01
 H1 = ef cd ab 89
 H2 = 98 ba dc fe
 20 H3 = 10 32 54 76

Core MD5

A=H0, B=H1, C=H2, D=H3

25 // Round 1.
 // Let [abcd k s i] denote the operation
 // $a = b + ((a + F(b,c,d) + W[k] + T[i]) \lll s)$.
 // Do the following 16 operations.

30 [ABCD 0 7 1] [DABC 1 12 2] [CDAB 2 17 3] [BCDA 3 22 4]
 [ABCD 4 7 5] [DABC 5 12 6] [CDAB 6 17 7] [BCDA 7 22 8]
 [ABCD 8 7 9] [DABC 9 12 10] [CDAB 10 17 11] [BCDA 11 22 12]
 [ABCD 12 7 13] [DABC 13 12 14] [CDAB 14 17 15] [BCDA 15 22 16]

-9-

```
// Round 2.
// Let [abcd k s i] denote the operation
// a = b + ((a + G(b,c,d) + W[k] + T[i]) <<< s).
// Do the following 16 operations.
```

5

```
[ABCD 1 5 17] [DABC 6 9 18] [CDAB 11 14 19] [BCDA 0 20 20]
[ABCD 5 5 21] [DABC 10 9 22] [CDAB 15 14 23] [BCDA 4 20 24]
[ABCD 9 5 25] [DABC 14 9 26] [CDAB 3 14 27] [BCDA 8 20 28]
[ABCD 13 5 29] [DABC 2 9 30] [CDAB 7 14 31] [BCDA 12 20 32]
```

10

```
// Round 3.
// Let [abcd k s i] denote the operation
// a = b + ((a + H(b,c,d) + W[k] + T[i]) <<< s).
// Do the following 16 operations.
```

15

```
[ABCD 5 4 33] [DABC 8 11 34] [CDAB 11 16 35] [BCDA 14 23 36]
[ABCD 1 4 37] [DABC 4 11 38] [CDAB 7 16 39] [BCDA 10 23 40]
[ABCD 13 4 41] [DABC 0 11 42] [CDAB 3 16 43] [BCDA 6 23 44]
[ABCD 9 4 45] [DABC 12 11 46] [CDAB 15 16 47] [BCDA 2 23 48]
```

20

```
// Round 4.
// Let [abcd k s i] denote the operation
// a = b + ((a + I(b,c,d) + W[k] + T[i]) <<< s).
// Do the following 16 operations.
```

25

```
[ABCD 0 6 49] [DABC 7 10 50] [CDAB 14 15 51] [BCDA 5 21 52]
[ABCD 12 6 53] [DABC 3 10 54] [CDAB 10 15 55] [BCDA 1 21 56]
[ABCD 8 6 57] [DABC 15 10 58] [CDAB 6 15 59] [BCDA 13 21 60]
[ABCD 4 6 61] [DABC 11 10 62] [CDAB 2 15 63] [BCDA 9 21 64]
```

30

H0 =H0+A, H1 =H1+B, H2 =H2+C, H3=H3+D

The information below sets out the so-called atomic operations which are required to perform the different algorithm calculations. The following steps indicate the

operation number, the operation performed, and the status of the read 140 and write 145 busses. Each operation listed below takes exactly one clock cycle.

SHA-1 ALGORITHM

5 initialization

	##	operation	Readbus	Writebus
	01.	A := H0	H0	(copy)
	02.	B := H1	H1	(copy)
	03.	C := H2	H2	(copy)
10	04.	D := H3	H3	(copy)
	05.	E := H4	H4	(copy)

0<=t<=15

	##	operation	Readbus	Writebus
15	01.	ACCU := B	B	(copy)
	02.	TMP := ACCU and C	C	(and)
	03.	ACCU := NOT B	B	(not)
	04.	ACCU := ACCU and D	D	(and)
	05.	ACCU := ACCU or TMP	TMP	(or)
20	06.	ACCU := ACCU + W[0]	W[0]	(+)
	07.	ACCU := ACCU + E	E	(+)
	08.	TMP := SL5(A)	A	(SL5)
	09.	ACCU := ACCU + TMP	TMP	(+)
	10.	TMP := ACCU + K[t]	K[t]	(+)
25	11.	E := D	D	(copy)
	12.	D := C	C	(copy)
	13.	C := SL30(B)	B	(SL30)
	14.	B := A	A	(copy)
	15.	A := TMP	TMP	(copy)
30	16.	ROTATE W[i]		

16<=t<=19

##	operation	Readbus	Writebus
01.	ACCU := B	B	(copy)

-11-

	02.	TMP := ACCU and C	C	(and)
	03.	ACCU := NOT B	B	(not)
	04.	ACCU := ACCU and D	D	(and)
	05.	TMP := ACCU or TMP	TMP	(or)
5	06.	ACCU := W[13]	W[13]	(copy)
	07.	ACCU := ACCU xor W[8]	W[8]	(xor)
	08.	ACCU := ACCU xor W[2]	W[2]	(xor)
	09.	ACCU := ACCU xor W[0]	W[0]	(xor)
	10.	W[0] := SL1	(ACCU)	(SL1)
10	11.	ACCU := W[0]	W[0]	(copy)
	12.	ACCU := ACCU + TMP	TMP	(+)
	13.	ACCU := ACCU + E	E	(+)
	14.	TMP := SL5(A)	A	(SL5)
	15.	ACCU := ACCU + TMP	TMP	(+)
15	16.	TMP := ACCU + K[t]	K[t]	(+)
	17.	E := D	D	(copy)
	18.	D := C	C	(copy)
	19.	C := SL30(B)	B	(SL30)
	20.	B := A	A	(copy)
20	21.	A := TMP	TMP	(copy)
	22.	ROTATE W[i]		

20<=t<=39 and 60<=t<=79

final round

	##	operation	Readbus	Writebus
25	01.	ACCU := A	A	(copy)
	02.	H0 := ACCU + H0	H0	(+)
	03.	ACCU := B	B	(copy)
	04.	H1 := ACCU + H1	H1	(+)
30	05.	ACCU := C	C	(copy)
	06.	H2 := ACCU + H2	H2	(+)
	07.	ACCU := D	D	(copy)
	08.	H3 := ACCU + H3	H3	(+)
	09.	ACCU := E	E	(copy)

-12-

10. H4 := ACCU + H4 H4 (+)

5 MD5 ALGORITHM

initialization

	##	operation	Readbus	Writebus
	01.	A := H0	H0	(copy)
	02.	B := H1	H1	(copy)
10	03.	C := H2	H2	(copy)
	04.	D := H3	H3	(copy)

Round 1 (16 iterations): $0 \leq i \leq 15$; $k=0$; $s=7,12,17,22,7,12,17,22 \dots$

	##	operation	Readbus	Writebus
15	01.	ACCU := B	B	(copy)
	02.	TMP := ACCU and C	C	(and)
	03.	ACCU := NOT B	B	(not)
	04.	ACCU := ACCU and D	D	(and)
	05.	TMP := ACCU or TMP	TMP	(or)
20	06.	ACCU := W[k]	W[k]	(copy)
	07.	ACCU := ACCU + A	A	(+)
	08.	ACCU := ACCU + T[i]	T[i]	(+)
	09.	TMP := ACCU + TMP	TMP	(+)
	10.	ACCU := SL[s](TMP)	TMP	(SL[s])
25	11.	TMP := ACCU + B	B	(+)
	12.	A := D	D	(copy)
	13.	D := C	C	(copy)
	14.	C := B	B	(copy)
	15.	B := TMP	TMP	(copy)
30	16.	ROTATE W[k]		

Preparation for Round 2

01. ROTATE W[k]

-13-

Round 2 (16 iterations): $16 \leq i \leq 31$; $k=1$; $s=5,9,14,20,5,9,14,20,5,\dots$

	## operation	Readbus	Writebus
	01. ACCU := B	B	(copy)
	02. TMP := ACCU and D	D	(and)
5	03. ACCU := NOT D	D	(not)
	04. ACCU := ACCU and C	C	(and)
	05. TMP := ACCU or TMP	TMP	(or)
	06. ACCU := W[k]	W[k]	(copy)
	07. ACCU := ACCU + A	A	(+)
10	08. ACCU := ACCU + T[i]	T[i]	(+)
	09. TMP := ACCU + TMP	TMP	(+)
	10. ACCU := SL[s] (TMP)	TMP	(SL[s])
	11. TMP := ACCU + B	B	(+)
	12. A := D	D	(copy)
15	13. D := C	C	(copy)
	14. C := B	B	(copy)
	15. B := TMP	TMP	(copy)
	16. ROTATE W[k]		
	17. ROTATE W[k]		
20	18. ROTATE W[k]		
	19. ROTATE W[k]		
	20. ROTATE W[k]		

Preparation for Round 3

	01. ROTATE W[k]
25	02. ROTATE W[k]
	03. ROTATE W[k]
	04. ROTATE W[k]

Round 3 (16 iterations): $32 \leq i \leq 47$; $k=5$; $s=4,11,16,23,4,11,16,\dots$

- 30 As an example of how the information above should be interpreted, step number 2 of the SHA-1 initialisation section relates to the operation $B := H1$, meaning that the register B is set to the value stored in H1. To achieve this, the tristate buffer 321 of register H1 and the tristate buffer 301 of the copy logic are enabled together. At the same time, the clock to register B is enabled, resulting in the data in H1 being written

into B. The tristate buffer control and clock signals are generated by the control circuit 400.

Similarly, step number 10 in the SHA-1 $0 \leq t \leq 15$ stage relates to the operation
5 $TMP := ACCU + K[t]$. The multiplexer and tristate buffer 332 is enabled for $K[10]$. The tristate buffer 304 is enabled for the ADD logic 215 and a gated clock signal is created and applied to the TMP register 120. In this way, the rising clock signal causes the sum of the data in $K[10]$ and ACCU to be written into the TMP register.

10 The last instruction in the $0 \leq t \leq 15$ stage for SHA-1 (and the $0 \leq i \leq 15$ stage for MD5) causes the entire W_i chain to be rotated, so that W_{14} is loaded with the data previously in W_{15} , W_{13} receives the data previously in W_{14} , and W_{15} receives the data previously in W_0 . Advantageously, this instruction may be implemented in parallel with the instruction above it (Step 15) as the rotate instruction does not
15 involve placing data onto the data bus. In this way, one clock cycle per iteration is saved, leading to a total saving of 80 cycles for SHA-1 and 64 cycles for MD5.

The embodiment presented has a bus width of 32 bits. However, it is possible to reduce the bus width to reduce the silicon area of the design at the expense of
20 operational speed. If the bus width is reduced to 16 bits, each 32 bit XOR operation, for example, will take two cycles rather than one cycle if a 32 bit bus was used.

In the light of the foregoing description, it will be clear to the skilled man that various modifications may be made within the scope of the invention.

25 The present invention includes and novel feature or combination of features disclosed herein either explicitly or any generalisation thereof irrespective of whether or not it relates to the claimed invention or mitigates any or all of the problems addressed.

CLAIMS

1. Apparatus arranged to accept digital data as an input, and to process said data according to one of either the Secure Hash Algorithm (SHA-1) or Message Digest (MD5) algorithm to produce a fixed length output word, said apparatus
5 including:

- a plurality of rotational registers for storing data, one of said registers being arranged to receive the input data; and
- data stores for initialisation of some of said plurality of registers according to
10 whether the SHA-1 or MD5 algorithm is used, said data stores including fixed data relating to SHA-1 and MD5 operation; and
- a plurality of dedicated combinatorial logic circuits arranged to perform logic operations on data stored in selected ones of said plurality of registers.

15 2. Apparatus as claimed in claim 1 wherein the register arranged to receive the input data is arranged to receive said input data serially.

3. Apparatus as claimed in claim 1 or 2 wherein the registers and combinatorial logic circuits are interconnected for communication via a pair of data busses.
20

4. Apparatus as claimed in claim 3 wherein the registers and combinatorial logic circuits are connected to write to a respective bus via respective tristate buffers.

5. Apparatus as claimed in any one of the preceding claims wherein the
25 apparatus includes a control circuit arranged to generate individually gated clock signals for each register.

6. Apparatus as claimed in claim 5 wherein said control circuit is further arranged to generate individual enabling signals to control the tristate buffers.
30

7. Apparatus as claimed in any one of the preceding claims wherein the rotational registers are arranged to be multiplexed prior to connection to a tristate buffer.

8. Apparatus as claimed in any one of the preceding claims wherein the combinatorial logic circuits include a copy circuit, a shift left circuit, a NOT circuit, an ADD circuit, an OR circuit, an AND circuit and an XOR circuit.

5

9. Apparatus as claimed in any one of the preceding claims wherein the apparatus is implemented as an integrated circuit.

10. Apparatus as claimed in any one of the preceding claims wherein the apparatus further includes circuitry arranged to perform digital signature creation or authentication.

10

1/2

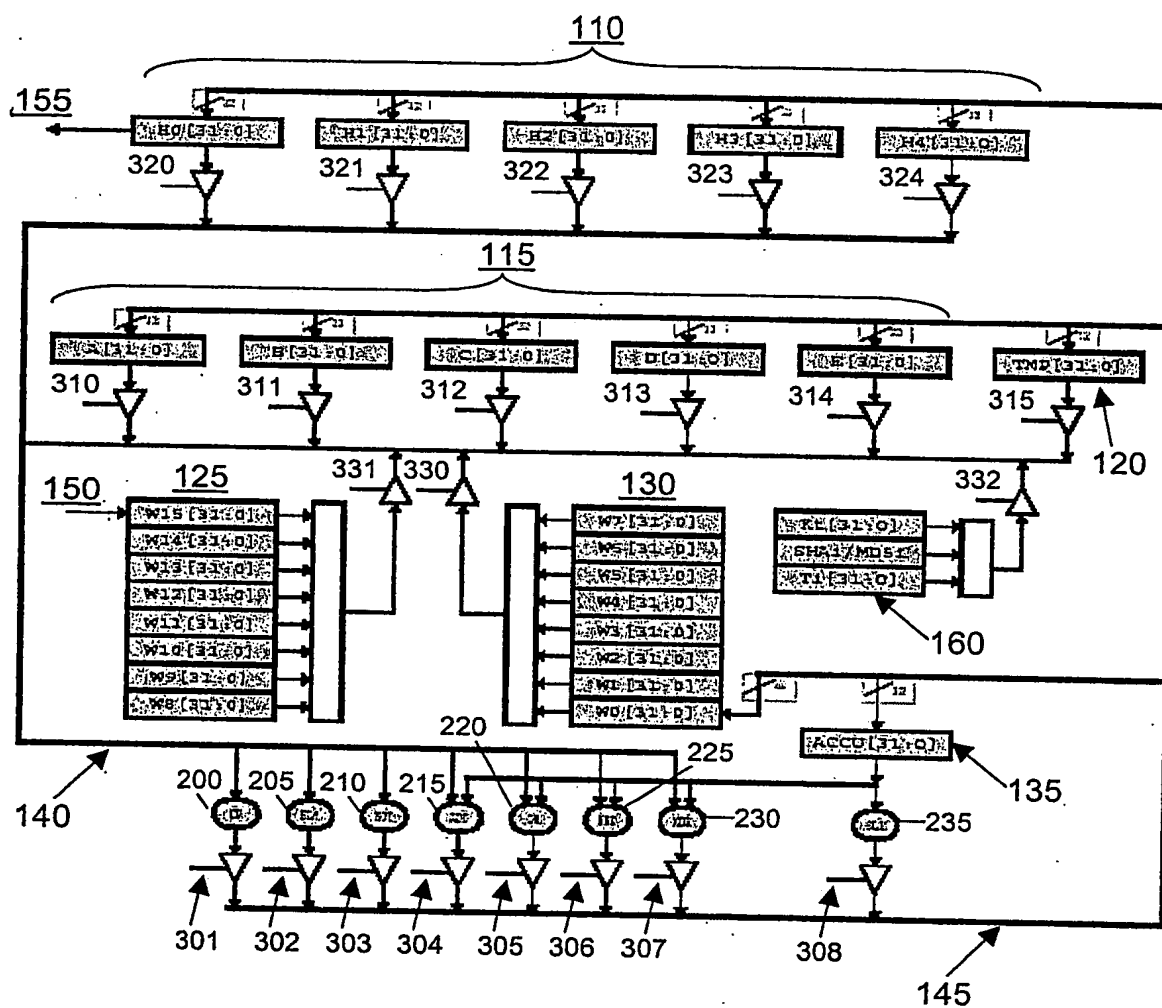


FIGURE 1

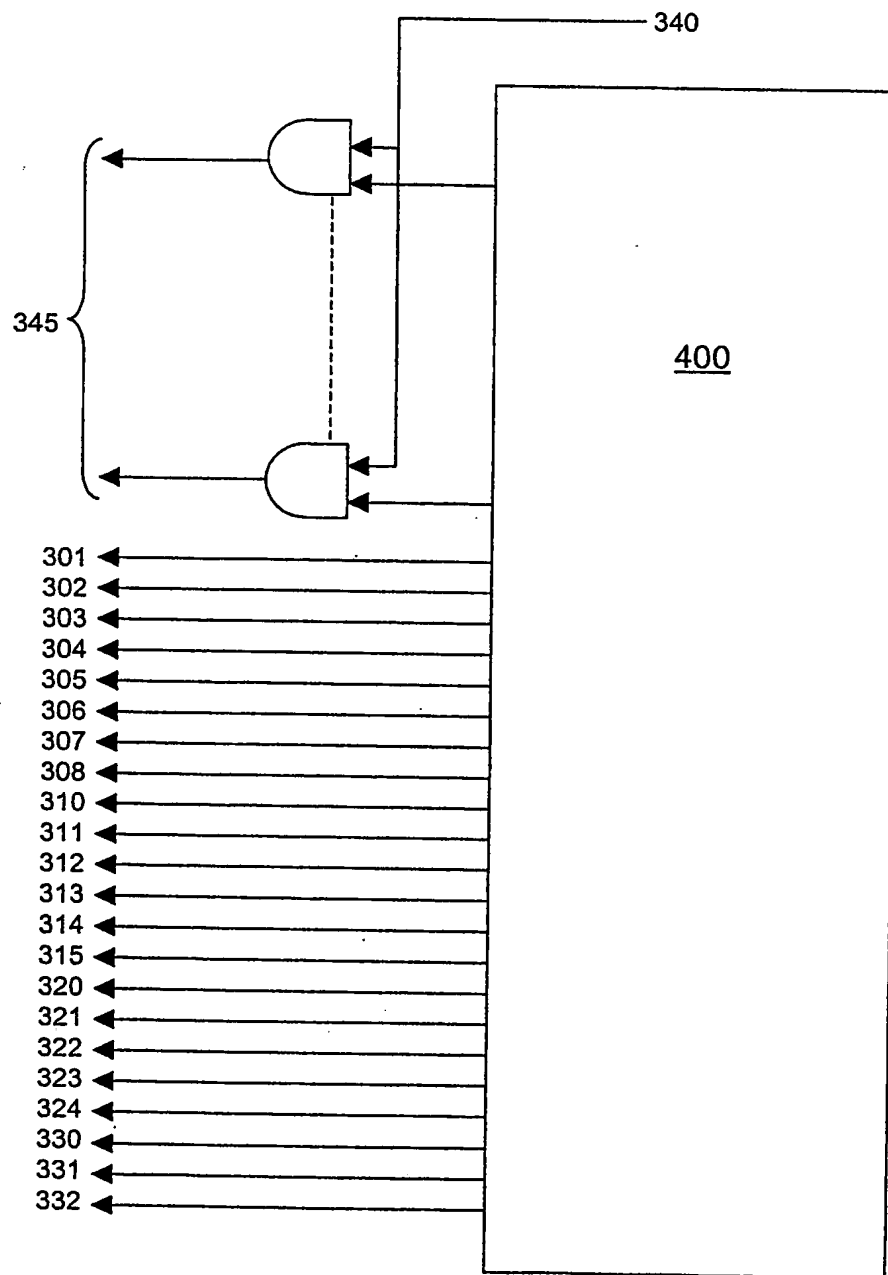


FIGURE 2

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT (PCT Article 36 and Rule 70)

REC'D 29 OCT 2004

WIPO PCT

Applicant's or agent's file reference ST/1012539PAT	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/SG 02/00245	International filing date (day/month/year) 21.10.2002	Priority date (day/month/year) 21.10.2002
International Patent Classification (IPC) or both national classification and IPC G06F17/10		
Applicant STMICROELECTRONICS ASIA PACIFIC PTE LTD et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 7 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

I ☒ Basis of the opinion

II ☐ Priority

III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability


IV ☐ Lack of unity of invention

V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

VI ☐ Certain documents cited

VII ☐ Certain defects in the international application

VIII ☐ Certain observations on the international application

Date of submission of the demand 27.04.2004	Date of completion of this report 28.10.2004
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Barba, M Telephone No. +49 89 2399-2732



**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/SG 02/00245**

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, Pages

1-14 as originally filed

Claims, Numbers

1-10 as originally filed

Drawings, Sheets

1-2 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
☐ the language of publication of the international application (under Rule 48.3(b)).
☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority in written form.
☐ furnished subsequently to this Authority in computer readable form.
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/SG 02/00245**

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	2-10
	No: Claims	1
Inventive step (IS)	Yes: Claims	
	No: Claims	2-10
Industrial applicability (IA)	Yes: Claims	1-10
	No: Claims	

2. Citations and explanations

see separate sheet

Reference is made to the following document:

D1: US 2002/066014 A1 (DWORKIN ET AL) 30 May 2002 (2002-05-30)

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

- 1 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of independent apparatus claim 1 is not new in the sense of Article 33(2) PCT, the reasons therefore being the following.
 - 1.1 The application concerns an implementation of the SHA-1 and MD5 algorithms by using a compact ASIC architecture, wherein the same hardware is used for both algorithms.

The apparatus of the application includes a plurality of shift registers (rotational registers) to receive the input data; registers to store constant values necessary to initialise the algorithms; a plurality of logic circuits coupled to the input registers by means of selection units (multiplexers).

Depending on the algorithm to be carried out the selection units configure the logic circuits accordingly and thereafter couple the logic circuits with the proper constant values. Tristate buffers are used to connect logic circuits with input registers. Individual clock signals are used for each register to reduce the power consumption.
 - 1.2 Document D1, which is provisionally considered as the closest prior art, discloses (see from paragraph 0004 to paragraph 0005; from paragraph 0009 to paragraph 0022; from paragraph 0023 to paragraph 0027) an apparatus for implementing multiple cryptographic hash algorithms such as SHA-1, MD4 and MD5. A register file is initialised to different data values; a logic circuit performs logical operations based on the selected cryptographic algorithm and provides a data value to a summing circuit that is summed with mode dependent constant values selected from registers, round and stepped generated data words to calculate the hash values for the stored input data.

In particular D1 discloses:

- i) a plurality of rotational registers for storing data, one of said registers being arranged to receive the input data (see from paragraph 0018 to paragraph 0020);
- ii) data stores for initialisation of some of said plurality of registers according to whether the SHA-1 or MD5 algorithm is used, said data stores including fixed data relating to SHA-1 and MD5 operation (see from paragraph 009 to paragraph 0017; paragraph 0022; from paragraph 0023 to paragraph 0027);
- iii) a plurality of dedicated combinatorial logic circuits arranged to perform logic operations on data stored in selected ones of said plurality of registers (see from paragraph 0012 to paragraph 0017; from paragraph 0019 to paragraph 0022; from paragraph 0024 to paragraph 0027).

1.3 Therefore, document D1 discloses an apparatus that includes features identical to the features of the apparatus of present independent claim 1.

The subject matter of claim 1 lacks novelty with regard to the apparatus known from D1 and, consequently, does not meet the requirements of novelty as set out in Article 33(2) PCT.

2 Dependent claims 2 to 4 and 6 to 10 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of inventive step, because the apparatus known from document D1 includes features that are equal or equivalent to the features of the apparatus of dependent claims 2 to 4 and claims 6 to 10 (see from paragraph 0004 to paragraph 0005; from paragraph 0009 to paragraph 0022; from paragraph 0023 to paragraph 0027).

Thus, the subject matter of dependent claims 2 to 4 lacks an inventive step contribution with regard to the apparatus known from D1 (Article 33 (3) PCT).

3 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of dependent claim 5 does not involve an inventive step in the sense of Article 33(3) PCT for the following reasons.

3.1 The apparatus according to claim 5 differs from that known from document D1 only in that the feature of individually generated gated clock signal has been omitted.

However, selecting common clock signal or individually generated clock signals is

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/SG 02/00245

merely one of several straightforward possibilities from which the skilled person would select, in accordance with circumstances, without the exercise of inventive skill (Article 33 (3) PCT).

- 4 With regard to the assessment of the present claims 1 to 10 on the question whether they are industrially applicable, the following is stated.
The subject matter of present claims 1 to 10 relates to an implementation of the SHA-1 and MD5 algorithms by using a compact ASIC architecture, wherein the same hardware is used for both algorithms, therefore it fulfills the requirements of industrial applicability as set out in Article 33 (4) PCT.
- 5 The application does not meet the requirements of Article 6 PCT, because claims 1 to 7 and 10 are not clear.
Some of the features in the apparatus claims 1 to 7 and 10 relate to a method of using the apparatus rather than clearly defining the apparatus in terms of its technical features. The intended limitations are therefore not clear from this claim, contrary to the requirements of Article 6 PCT.
In order to remedy this anomaly, a formulation of the claims in terms of functional means ("means adapted to") should be used.
- 6 Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the document D1 is not mentioned in the description, nor is this document identified therein.
 - 6.1 Independent claim 1 is not in the two-part form in accordance with Rule 6.3(b) PCT, which in the present case would be appropriate, with those features known in combination from the prior art (document D1) being placed in the preamble (Rule 6.3(b)(I) PCT) and with the remaining features being included in the characterising part (Rule 6.3(b)(ii) PCT).
 - 6.2 The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).
 - 6.3 Furthermore, at page 14, last paragraph, the description contains general statements that the extent of protection may be expanded in some vague and not

INTERNATIONAL PRELIMINARY

International application No. PCT/SG 02/00245

EXAMINATION REPORT - SEPARATE SHEET

precisely defined way. Such general statements shall be deleted as contrary to Article 6 PCT, cf. also PCT Preliminary Examination Guidelines, C-III, 4.3a.

INTERNATIONAL SEARCH REPORT

Rec'd PCT/PTO 18 APR 2005

International Application No

PCT/SG 02/00245

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC, WPI Data, PAJ, IBM-TDB, COMPENDEX, SCISEARCH

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/066014 A1 (DWORKIN ET AL) 30 May 2002 (2002-05-30) page 3, left-hand column, line 23 -right-hand column, line 27 page 1, left-hand column, line 9, paragraph 9 -page 2, right-hand column, line 22	1-4, 7-10
A	page 1, left-hand column, paragraph 4 - paragraph 5	5, 6
A	US 5 778 069 A (SIMON DANIEL R ET AL) 7 July 1998 (1998-07-07) column 6, line 61 -column 7, line 20 column 5, line 30 -column 6, line 45 -/--	1-10

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"Z" document member of the same patent family

Date of the actual completion of the international search

27 December 2002

Date of mailing of the international search report

15/01/2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Barba, M

INTERNATIONAL SEARCH REPORT

International Application No

PCT/SG 02/00245

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"SHA-256 Crypt Core Family" HDL DESIGN HOUSE, 'Online! August 2001 (2001-08), pages 1-2, XP002226135 Retrieved from the Internet: <URL:http://www.hdl-dh.com> 'retrieved on 2002-12-27! page 1, line 10 - line 27 page 2, line 7 - line 35 ----	1-10
A	"SHA-1 High Performance Hash Function" ALMA TECHNOLOGIES, 'Online! May 2002 (2002-05), pages 1-3, XP002226136 Retrieved from the Internet: <URL:http://www.alma-tech.com> 'retrieved on 2002-12-27! page 1, line 15 - line 29 -----	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/SG 02/00245

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 2002066014	A1	30-05-2002	NONE	
US 5778069	A	07-07-1998	NONE	

RECD 15 JAN 2003

WIPO

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference ST/1012539	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/SG 02/00245	International filing date (day/month/year) 21/10/2002	(Earliest) Priority Date (day/month/year)
Applicant STMICROELECTRONICS ASIA PACIFIC PTE LTD		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 04 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

- a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

- b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. ☐ **Certain claims were found unsearchable** (See Box I).

3. ☐ **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

☐ the text is approved as submitted by the applicant.

☒ the text has been established by this Authority to read as follows:

APPARATUS TO IMPLEMENT DUAL HASH ALGORITHM

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No.

☐ as suggested by the applicant.

☒ because the applicant failed to suggest a figure.

☐ because this figure better characterizes the invention.

1
☐ None of the figures.